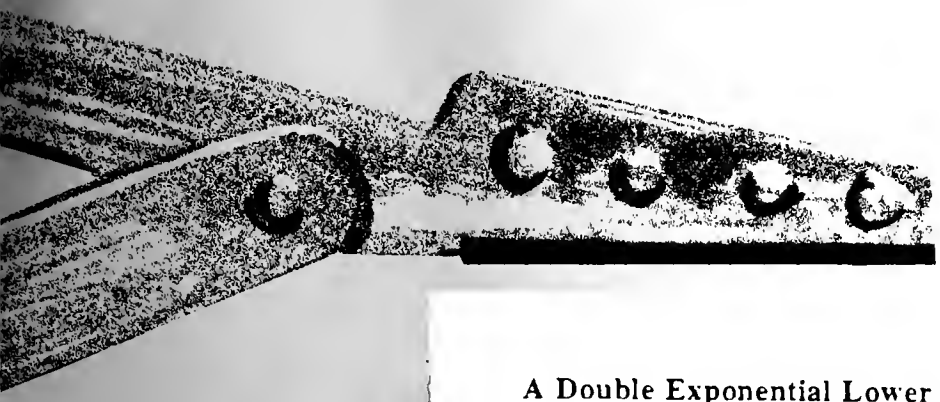
Robotics Research Technical Report



A Double Exponential Lower Bound for Degree-compatible Gröbner Bases

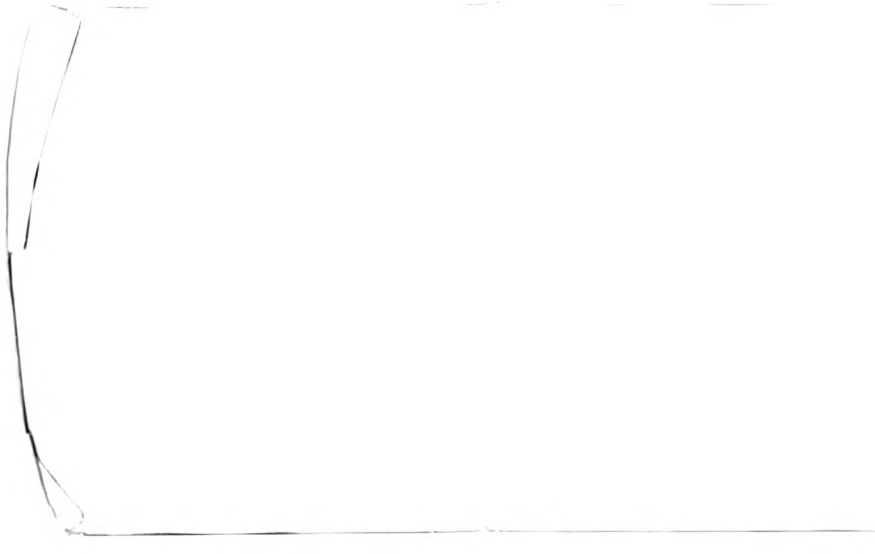
by

Chee K. Yap

Technical Report No. 415
Robotics Report No. 181
November, 1988

New York University
Courant Institute of Mathematical Sciences

Computer Science Division
251 Mercer Street New York, N.Y. 10012



A Double Exponential Lower Bound for Degree-compatible Grōbner Bases

by

Chee K. Yap

Technical Report No. 415
Robotics Report No. 181
November, 1988

New York University
Dept. of Computer Science
Courant Institute of Mathematical Sciences
251 Mercer Street
New York, New York 10012

Work on this paper has been supported in part by NSF Grants DCR-84-01898, CCR-87-03458 and ONR Grant N00014-85-K-0046. This report is simultaneously released as a technical report of *Fachbereich Mathematik*, Freie University, Berlin.

A Double Exponential Lower Bound for Degree-compatible Gröbner Bases

Chee K. Yap
Courant Institute of Mathematical Sciences
New York University
251 Mercer Street
New York, NY 10012

and

Fachbereich Mathematik,
Freie Universität Berlin,
Arnimallee 206,
D-1000 Berlin

Abstract

We describe an ideal $J_{n,d}$ generated by $O(n)$ polynomials of degree $d + O(1)$ over $4n$ variables such that every Gröbner basis for $J_{n,d}$ with respect to degree-compatible orderings has maximum degree $\geq d^{2^{n-1}}$.

1 Introduction

This paper is a sequel to [8].

In the former paper, we constructed a commutative Thue system with $\sim 2n$ variables and $O(n)$ rules, each rule of length $d+O(1)$ that 'counts' to d^{2^n}. It has been realized since the papers of Huynh [4] and Mora-Möller [7] that from such systems, one can construct a set of polynomials F such that any Gröbner basis for F (with respect to some degree-compatible admissible ordering) has maximum degree that is double exponential in n. The relevant theorems (the cited papers contain other results of independent interest) in these two papers are somewhat dissatisfactory as explained in [8]. The present paper is an attempt to correct this.

It should be noted that there is as yet no general theorem that shows that any Thue system which 'counts' to d^{2^n} with the above parameters will automatically yield the kind of double exponential behaviour we desire. Hence one must exploit particular properties of such a Thue system. As in most lower bound results, determining which properties to exploit can often be an illusive search. Since the underlying construction in Yap [8] is simpler than the Mayr-Meyer construction [5], we would expect that a complete proof based on our construction to be simpler than those attempted in [4] and [7].

Our lower bound is also a qualitative improvement on [4], [7] since our construction uses fewer variables than that of Mayr-Meyer. This qualitative improvement is important in the research effort to determine the asymptotic worst case behaviour of Gröbner basis. The recent result of Dubé [3] shows that any Gröbner basis G on n variables has maximum degree at most d^{2^n}, where d is the degree bound on any set of generators for (G). The result in the present paper shows that the maximum degree of G can essentially attain $d^{2^{n/4}}$, assuming a degree-compatible admissible ordering. There are as yet no lower bounds for other admissible orderings.

This paper assumes the preliminary section of [8]; some familiarity with the construction of the Thue systems S_0 and S_1 as well as the Basic Lemma found there is expected. The rest of this paper is organized as follows:

In Section 2, we prove the Value Lemma which is a fundamental tool for estimating the degrees of assertions of S_0. In Section 3, we prove that the set of assertions of S_0 forms a tree T_0. In Section 4, we consider some basic properties of Gröbner bases formed from Thue ideals (i.e. ideals formed from Thue systems). In Section 5, we prove that the reduced Gröbner basis G_0 formed from S_0 must have double-exponential degree, assuming a degree-compatible admissible ordering. In Section 6, we modify S_0 to a Thue system S_1' which yields the result stated in our abstract. We conclude in Section 7.

2 The Value Lemma

Recall from [8] that the Thue system S_0 has the following six (forward) rules and their reverses:

Start Rules. $(k = 1, 2, \ldots, n)$

$$(\mathrm{S1})_k \quad A_0 \xrightarrow{Q_{\mathtt{start}} F_{1,k}[\mathtt{pass}] F_k[\mathtt{inc}]} B_0 A_k^d \quad (\text{"increment rule"})$$

$$(\mathrm{S2})_k \quad A_0 B_k^d \xrightarrow{Q_{\mathtt{start}} F_{1,k}[\mathtt{pass}] F_k[\mathtt{dec}]} B_0 \quad (\text{"decrement rule"})$$

$$(\mathrm{S3}) \quad Q_{\mathtt{start}} B_0^d \longrightarrow Q_{\mathtt{finish}} \quad (\text{"finish rule"})$$

Finish Rules. $(k = 1, 2, \ldots, n-1)$

$$(\mathrm{F1})_k \quad Q_{\mathtt{finish}} F_{1,k}[\mathtt{dec}] F_k[\mathtt{inc}] \longrightarrow Q_{\mathtt{start}} A_0^d F_{1,k}[\mathtt{inc}] F_k[\mathtt{pass}]$$
("inc ⇒ pass rule")

$$(\mathrm{F2})_k \quad Q_{\mathtt{finish}} F_{1,k}[\mathtt{dec}] A_k \xrightarrow{F_k[\mathtt{pass}]} Q_{\mathtt{start}} A_0^d F_{1,k}[\mathtt{inc}] B_k$$
("pass ⇒ pass rule")

$$(\mathrm{F3})_k \quad Q_{\mathtt{finish}} F_{1,k}[\mathtt{dec}] F_k[\mathtt{pass}] A_k \longrightarrow Q_{\mathtt{start}} A_0^d F_{1,k}[\mathtt{inc}] F_k[\mathtt{dec}] B_k$$
("pass ⇒ dec rule")

Also recall the initial assertion w_0 is given by $Q_{\mathtt{start}} A_0^d F_{1,n+1}[\mathtt{inc}]$.

In this section we prove a very useful tool for estimating the A_k- and B_k-degrees of assertions for the system S_0.

Definition

An interval $[j,k], 1 \le j \le k \le n$, is called a *block* of an assertion w if $F_{j,k}[\mathtt{pass}] \mid w$ but for all intervals $[j',k']$ that properly contain $[j,k]$, we have $F_{j',k'}[\mathtt{pass}] \nmid w$. The *value* of a block $[j,k]$ of w is defined by:

$$V_w(j,k) = \sum_{i=j}^{k-1} e(i) \cdot \deg_{B_i}(w) + \begin{cases} e(0) \cdot \deg_{B_0}(w) & \text{if } j = 1,\ Q_{\mathtt{start}} \mid w, \\ e(1) & \text{if } j = 1,\ Q_{\mathtt{finish}} \mid w, \\ 0 & \text{if } j > 1,\ F_{j-1}[\mathtt{inc}] \mid w, \\ e(j-1)(e(j-1) - \deg_{A_{j-1}}(w)) & \text{if } j > 1,\ F_{j-1}[\mathtt{dec}] \mid w. \end{cases}$$

Note: For any assertion w, there are integers

$$0 = k_0 < k_1 < k_2 < \ldots < k_r = n$$

such that $[1, k_1], [k_1 + 1, k_2], \ldots, [k_{r-1} + 1, k_r]$ are the blocks of w. Call $[k_{i-1} + 1, k_i]$ the i^{th} *block* of w. Also, let $\deg_k(w)$ denote $\deg_{A_k}(w) + \deg_{B_k}(w)$.

Value Lemma

Let w be an assertion obtained by applying only forward rules to the initial assertion w_0.

(a) For any $k = 1, \ldots, n$, if $F_k[\texttt{inc}] \mid w$ then $\deg_{B_k}(w) = 0$

(b) For any block $[j, k]$ of w,

$$\deg_k(w) = \begin{cases} V_w(j,k) & \text{if } F_k[\texttt{inc}] \mid w \ , \\ e(k) - V_w(j,k) & \text{if } F_k[\texttt{dec}] \mid w \ . \end{cases}$$

(c) For any $k = 1, \ldots, n$, if $F_k[\texttt{pass}] \mid w$ then $\deg_k(w) = e(k)$.

Proof of Value Lemma

The lemma holds at $w = w_0$. We now show that if the lemma holds at w' and $w' \rightarrow w$ is a forward transition then it holds at w. If this transition were an application of a start rule, this is easy to see. We next consider the finish rules in detail.

Case Rule (F1)

We consider parts (a), (b) and (c) of the lemma.

(a) It suffices to check that $\deg_{B_i}(w) = 0$ for $i = 1, \ldots, k-1$. Note that $[i, i]$ is a block of w and also of w'. Since $\deg_{B_i}(w) = \deg_{B_i}(w')$, what we want to check is a consequence of the stronger statement

$$\deg_i(w') = 0 \text{ and } V_{w'}(i,i) = e(i).$$

We use induction on i. If $i = 1$, $V_{w'}(1,1) = e(1)$ by definition, and $\deg_1(w') = e(1) - V_{w'}(1,1) = 0$. If $i > 1$, $V_{w'}(i,i) = e(i-1)(e(i-1) - \deg_{A_{i-1}}(w')) = e(i)$. Hence $\deg_i(w') = e(i) - V_{w'}(i,i) = 0$.

(b) It suffices to check the lemma for the first k blocks of w. The first $(k-1)$ blocks of w and of w' are $[i, i]$, for $i = 1, \ldots, k-1$. Now $V_{w'}(i,i) = e(i)$ as shown in part (a), and $V_w(i,i) = 0$ by definition. Hence $\deg_i(w) = \deg(w') = e(i) - V_{w'}(i,i) = 0 = V_w(i,i)$, as desired. Now consider the k^{th} block of w. This is $[k, \ell]$ if the $(k+1)^{\text{st}}$

block of w' is $[k+1, \ell]$. Since $\deg_\ell(w) = \deg_\ell(w')$, the lemma holds for the k^{th} block $[k, \ell]$ provided $V_w(k, \ell) = V_{w'}(k+1, \ell)$. To see this,

$$\begin{aligned} V_w(k,\ell) &= \sum_{i=k}^{\ell-1} e(i) \cdot \deg_{B_i}(w) \\ &= \sum_{i=k+1}^{\ell-1} e(i) \cdot \deg_{B_i}(w') \end{aligned}$$

since $\deg_{B_i}(w) = \deg_{B_i}(w')$ for all i and $\deg_{B_k}(w') = 0$ by the induction hypothesis (a). But the latter expression gives us the definition of $V_{w'}(k+1, \ell)$, as desired.

(c) We only need to check that

$$\deg_k(w) = e(k).$$

But $\deg_k(w) = \deg_k(w') = V_{w'}(k,k) = e(k-1)(e(k-1) - \deg_{A_{k-1}(w')}) = e(k)$ since $\deg_{A_{k-1}}(w) \leq \deg_{k-1}(w') = 0$ by the proof in part (a).

Case Rule (F2)

(a) This is similar to rule (F1).

(b) For some $\ell \geq k$, $[k, \ell]$ is the k^{th} block of w as well as of w'. To show the lemma for this block, it suffices to prove $V_w(k, \ell) = V_{w'}(k, \ell)$.
But

$$V_w(k,\ell) = \sum_{i=k}^{\ell-1} e(i) \cdot \deg_{B_i}(w)$$

and

$$\begin{aligned} V_{w'}(k,\ell) &= \sum_{i=k}^{\ell-1} e(i) \cdot \deg_{B_i}(w') + (e(k-1)(e(k-1) - \deg_{A_{k-1}}(w')) \\ &= \sum_{i=k}^{\ell-1} e(i) \cdot \deg_{B_i}(w') + e(k) \end{aligned}$$

since $\deg_{k-1}(w') = 0$. The equality $V_w(k, \ell) = V_{w'(k,\ell)}$ follows from the observation

$$\deg_{B_i}(w) = \begin{cases} \deg_{B_i}(w') & \text{if } i \neq k, \\ 1 + \deg_{B_i}(w') & \text{if } i = k. \end{cases} \quad (1)$$

The lemma (part b)) holds for all the other blocks using the same reasoning as for Rule (F1). This part holds at w since the lemma holds at w'.

Case Rule (F3)

(a) As before.

(b) If $[k,\ell]$ is the k^{th} block of w', this divides into the k^{th} and $(k+1)^{\text{st}}$ blocks, $[k,k]$ and $[k+1,\ell]$, of w. For the k^{th} block of w,

$$\begin{aligned} V_w(k,k) &= 0, \\ \deg_k(w') &= e(k) \qquad \text{(by induction hypothesis (c)).} \end{aligned}$$

Hence $\deg_k(w) = \deg_k(w') = e(k) - V_w(k,k)$, as desired. For the $(k+1)^{\text{st}}$ block, it suffices to show

$$V_w(k+1,\ell) = V_{w'}(k,\ell).$$

Now

$$\begin{aligned} V_w(k+1,\ell) &= \sum_{i=k+1}^{\ell-1} e(i) \cdot \deg_{B_i}(w), \\ V_{w'}(k,\ell) &= \sum_{i=k}^{\ell-1} e(i) \cdot \deg_{B_i}(w') + e(k). \end{aligned}$$

These two expressions are equal since equation (1) above holds.

(c) This part follows immediately under the assumption that the lemma holds at w'.

QED

Recall that a derivation is said to be mixed if it involves both forward and reverse transitions.

Corollary 1 *Assertions derived from w_0 using simple mixed derivations are disjoint from those derived from w_0 using forward derivations.*

Proof:

If $w_0 \xrightarrow{*} w$ via a simple mixed derivation, it is easily checked (cf. [8]) that $B_k F_k[\mathtt{inc}] \mid w$ for some $k = 1, \ldots, n-1$. The Value Lemma (part (a)) shows that such w cannot be obtained from forward derivations.

QED

Another consequence of the Value Lemma useful for the application of the Basic Lemma is this.

Corollary 2 *Let w be derived from w_0 via a forward derivation. If $Q_{\texttt{finish}}F_{1,k}[\texttt{dec}] \mid w$ $(k = 1, \ldots, n)$ then $\deg_i(w) = 0$ for $i = 0, \ldots, k-1$.*

Proof

It is easy to see that $\deg_0(w) = 0$. For $i > 0, \deg_i(w) = e(i) - V_w(i,i) = 0$ since $V_w(i,i) = e(i) - e(i-1) \cdot \deg_{A_{i-1}}(w)$ and $\deg_{A_{i-1}}(w) \leq \deg_{i-1}(w) = 0$ by induction on i.

QED

3 Mistakes and the Assertion Tree

Our goal is to show that the set of all assertions of S_0 forms a tree rooted at w_0 and to give some insights into the structure of this tree.

Let w be well-formed. A transition $w \rightarrow w'$ is called a *mistake at level k* if it is an application of

(a) Rule $(\text{F3})_k$ when $\deg_{A_k}(w) \geq 2$

(b) Rule $(\text{F2})_k$ when $\deg_{A_k}(w) = 1$

(c) reverse of Rule $(\text{F1})_k$.

We call the mistake a *forward* (resp. *reverse*) mistake in case (a) or (b) (resp. (c)). The *signature* of the forward mistake $w \rightarrow w'$ is (k, m) where $\deg_{A_k}(w) = m$. So $m = 1$ iff the mistake is type (b). For completeness, we also define the signature of a reverse mistake at level k to be $(k, 0)$. Furthermore, observe that in any simple derivation, the first application of a reverse rule is necessarily a mistake.

We had in the first paper observed that after a reverse mistake has occurred, any simple derivation can only continue for at most $d+1$ steps and these can only use reverse rules. Furthermore, the continuation is unique. We record these remarks in:

Lemma 1 *Every simple derivation D starting from w_0 consists of two parts D_1 and D_2 where $D = D_1 D_2$, D_1 is a forward and D_2 is a backward derivation. Here, D_2 may be empty. Moreover, D contains a reverse mistake iff D_2 is non-empty.*

QED

Lemma 2 *Let $1 \leq k \leq \ell \leq n$. In any simple derivation from w_0, after a mistake at level k, the finish rules $(\mathrm{F1})_\ell$, $(\mathrm{F2})_\ell$ and $(\mathrm{F3})_\ell$ cannot subsequently be applied.*

Proof

This is true if the mistake is a reverse mistake. So suppose it is a forward mistake with signature (k,m). If the mistake is $w \rightarrow w'$ then by the Value Lemma,

$$\deg_k(w') = e(k).$$

If any of the rules $(\mathrm{F1})_\ell$, $(\mathrm{F2})_\ell$ or $(\mathrm{F3})_\ell$ were applied subsequently to an assertion w'' then

$$Q_{\mathtt{finish}} F_{1,k}[\mathtt{dec}]|w''.$$

Let w''' be the first assertion after w' where $Q_{\mathtt{finish}} F_{1,k}[\mathtt{dec}]|w'''$. By the corollary to the Value Lemma,

$$\deg_i(w''') = 0 \text{ for } i = 0, \ldots, k-1.$$

This implies by the Basic Lemma that the subderivation from w' to w''' is a standard derivation at level k.

There are two cases.

Case 1 The signature (k,m) is in fact $(k,1)$. Then $Q_{\mathtt{finish}} F_{1,k}[\mathtt{dec}] F_k[\mathtt{pass}]|w'''$ but $A_k \nmid w'''$. Then no rule is applicable to w''', contradiction.

Case 2 In the signature (k,m), we have $m \geq 2$. The subderivation from w' to w''' is a standard derivation and $F_k[\mathtt{dec}]|w'$. The Basic Lemma (part b) implies that $\deg_{B_k}(w') \geq e(k)$. But this yields a contradiction since

$$\begin{aligned} \deg_{B_k}(w') &= \deg_k(w') - \deg_{A_k}(w') \\ &= e(k) - (m-1) < e(k). \end{aligned}$$

QED

Corollary 3 *Let D be any simple derivation from w_0. If D contains r mistakes where the i^{th} mistake occurs at level $k(i)$ then*

$$k(1) > k(2) > \cdots > k(r).$$

Furthermore, all except possibly the last mistake is a reverse mistake.

Proof

It is clear that after a reverse mistake, no other mistakes can happen. Assume the corollary is false. So for some $i = 1, \ldots, r-1$, the i^{th} mistake is a forward mistake and

$k(i) \leq k(i+1)$. Hence the $(i+1)^{\text{th}}$ mistake is an application of rule $(\mathrm{F}j)_{k(i+1)}$ $(j = 1,2,3)$. This is impossible by the previous lemma.

QED

Define for any word w,

$$\Delta(w) = \sum_{k=0}^{n} (\deg_{A_k}(w) - \deg_{B_k}(w))$$

Lemma 3 *If $w \xrightarrow{\bullet} w'$ by a forward derivation then $\Delta(w') > \Delta(w)$.*

Proof

We only have to check this for a single transition, $w \rightarrow w'$. But it is easily seen that $\Delta(w') > \Delta(w)$ for each of the start and finish rules.

QED

Corollary 4 *Let D be any simple derivation from w_0. Then D is repetition-free.*

Proof

Divide D into D_1, D_2 where D_1 (resp. D_2) is a forward (resp. reverse) derivation. There is no repetition in D_1 (otherwise we get two occurrences of a word $w \in D_1$, with $w \xrightarrow{\bullet} w$ and $\Delta(w) > \Delta(w)$). It is easy to see that D_2 also has no repetition. D is repetition free since D_1 and D_2 are disjoint.

QED

Theorem 1 *For any assertion w, there is exactly one simple derivation from w_0 to w.*

Proof

There are two ways in which a simple derivation $D : w_0 \rightarrow \cdots \rightarrow w_m = w$ may not be uniquely determined by w. Either (a) D can be extended into a simple but repetitious derivation

$$D_1 : w_0 \rightarrow \cdots \rightarrow w_m \rightarrow w_{m+1} \rightarrow \cdots \rightarrow w_p$$

for some $p > m$ and $w_p = w_m = w$ or else (b) there is another simple derivation

$$D_2 : w_0 \to u_1 \to u_2 \to \cdots \to u_q = w$$

and $D \neq D_2$ but neither derivation is a prefix of the other. We had shown (a) impossible. If (b) holds, we may assume without loss of generality that $w_{m-1} \neq u_{q-1}$. There are 3 cases.

(i) One transition $w_{m-1} \to w$ is forward and the other $w_{p-1} \to w$ is reverse. This contradicts the result that assertions reached by forward derivations are disjoint from that which has some reverse transition.

(ii) Both transitions $w_{m-1} \to w$ and $w_{p-1} \to w$ are forward transitions. This means one is an application of $(\mathrm{F1})_k$ and the other an application of $(\mathrm{F2})_k$. If $w_{m-1} \to w$ is an application of $(\mathrm{F2})_k$ then $w_0 \to \cdots \to w_{m-1} \to w \to u_{p-1}$ is a simple derivation. Hence u_{p-1} is reached by forward as well as by mixed derivations, contradiction.

(iii) Both transitions are reverse transitions. This means one is an application of reverse (F2) and the other an application of reverse (F3). This means that $w_0 \to \cdots \to w_m \to w \to u_{p-1}$ is a simple derivation consisting of three parts: a forward derivation followed by a reverse derivation followed by a forward derivation. Each part is non-empty. This contradicts the fact that simple derivations have at most two parts, a forward followed by a reverse derivation.

QED

We form a tree T_0 whose nodes consist of all assertions of S_0 and the edges of T_0 are (w, w') where the unique simple derivation from w_0 to w' has w as the penultimate word. Hence w_0 is the root and w_∞ are among the leaves of T_0. Call T_0 the *tree of assertions.* The 'trunk' of T_0 is the mistake-free derivation from w_0 to w_∞. All other branches of T_0 are offshoots from this trunk caused by mistakes. Moreover, each branch is uniquely characterized by the signatures of its mistakes. Finally note that for any two assertions w_1 and w_2, there is a unique simple derivation $D : w_1 \stackrel{*}{\to} w_2$. We write $\mathtt{distance}(w_1, w_2)$ for the number of transitions in D.

4 Gröbner Bases of Thue Ideals

Given a commutative Thue system (Σ, S), we may form a set of polynomials $F_S \subseteq \mathbf{Q}[\Sigma]$ where $(\alpha, \beta) \in S$ iff $\beta - \alpha \in F_S$. We call polynomials of the form $\beta - \alpha$ *Thue polynomials* and an ideal generated by such polynomials *Thue ideals.*

For a background on Gröbner bases, see for example [1] [6]. We fix $\lesssim_{\mathcal{A}}$ to be any admissible ordering (i.e. $\lesssim_{\mathcal{A}}$ is a total ordering on $\Sigma^\oplus$ such that for all $u, v, w \in \Sigma^\oplus$, $1 \lesssim_{\mathcal{A}} w$ and

$u \lesssim_{\lambda} v \Rightarrow uw \lesssim_{\lambda} vw$.) For any polynomial $f = f_1 + f_2 + \cdots + f_k$ where f_i are monomials, and $f_1 \lesssim_{\lambda} f_2 \lesssim_{\lambda} \cdots \lesssim_{\lambda} f_k$ (the ordering $\lesssim_{\lambda}$ is extended to monomials by ignoring the coefficients) we define $\texttt{Hterm}(f) = f_1$.

Among the (finite) generating sets for an ideal $I \subseteq \mathbf{Q}[\Sigma]$ those sets known as *Gröbner bases* for I have particularly nice computational properties. Here we use the following characterization for a set $G \subseteq I$ to be a Gröbner basis for I:

Let $G = \{g_1, \ldots, g_m\}$. For all $f \in I$ there exists polynomials $f_1, \ldots, f_m$ such that

$$f = \sum_{i=1}^{m} g_i f_i \text{ and } \texttt{Hterm}(f) \lesssim_{\lambda} \texttt{Hterm}(g_i f_i) \text{ for all } i.$$

In this paper, we are only interested in admissible orderings that are *degree-compatible* (also called *total-degree orderings*), that is, for $u, v \in \Sigma^{\oplus}$, $\deg(u) < \deg(v)$ implies $u \lesssim_{\lambda} v$.

A basic concept of Gröbner basis theory is the *reduction relation*. If f, h are polynomials, a set of polynomials, we write

$$f \succ h \pmod{G}$$

if for some $g \in G$, and some monomial α, $\alpha\texttt{Hterm}(g)$ is a monomial of f and $h = f - \alpha g$. We say f is *reducible* by G in this case. A Gröbner basis G is *reduced* if for each $g \in G$, $\texttt{Hterm}(g)$ is monic (i.e. coefficient is 1) and g is not reducible by $G - \{g\}$. Buchberger has shown that the reduced Gröbner bases for an ideal is unique, once the admissible ordering is fixed.

Lemma 4 *If G is the reduced Gröbner basis for a Thue ideal then G consists of Thue polynomials.*

Proof (**Note:** this proof is not self-contained in this paper and holds for any admissible ordering.)

Let the Thue ideal be generated by the set F of Thue polynomials. Applying a suitable version of Buchberger's algorithm to F gives us the unique reduced gröbner basis G for (F). Each member of $G - F$ is obtained as the S-polynomial (not defined here) of two previously computed polynomials. By induction on the number of steps in Buchberger's algorithm, computed polynomial in G is Thue (using the fact that the S-polynomial of two Thue polynomials is still Thue).

QED

A derivation $(w_1, w_2, \cdots, w_m)$ is *descending* if $w_m \lesssim_{\lambda} w_{m-1} \lesssim_{\lambda} \cdots \lesssim_{\lambda} w_1$.

Lemma 5 *Let S be any Thue system and G the corresponding reduced Gröbner basis for F_S. Let $v_1 \underset{A}{\leq} u_1$ be words. If $u_1 - v_1 \in (G)$ then there exists two descending derivations*

$$u_1 \rightarrow u_2 \rightarrow \cdots \rightarrow u_p \,(\mathrm{mod} S)$$

$$v_1 \rightarrow v_2 \rightarrow \cdots \rightarrow v_q \,(\mathrm{mod} S)$$

where $p \geq 2, q \geq 1$, and $u_p = v_q$.

Proof

$u_1 - v_1 \in (G)$ implies $u_1 - v_1 = \sum_{i=1}^{r} \alpha_i g_i$ where $G = \{g_1, \ldots, g_r\}$ and α_i are polynomials such that $u_1 = \mathtt{Hterm}(u_1 - v_1) \underset{A}{\leq} \mathtt{Hterm}(\alpha_i g_i)$ for all i. This means that for some constant $c \in \mathbf{Q}$, $cu_1 = \mathtt{Hterm}(\alpha_i g_i)$ for some i. If $g_i = u_2' - v_2', v_2' \underset{A}{\leq} u_2'$, then for some word β_2, we get $u_2'\beta_2 = u_1$. Let $u_2 = v_2'\beta_2$. Hence (u_1, u_2) is a descending derivation $(\mathrm{mod} S)$ and $u_2 - v_1 = (u_1 - v_1) - \beta_2(u_2' - v_2') \in (G)$. If $u_2 = v_1$ then our lemma is proved (with $p = 2$, $q = 1$). Otherwise, we can repeat the argument using the polynomial $u_2 - v_1$ in place of $u_1 - v_1$. In general, we have constructed two descending derivations $u_1 \rightarrow u_2 \rightarrow \ldots \rightarrow u_p$ and $v_1 \rightarrow v_2 \rightarrow \ldots \rightarrow v_q$ with $u_p - v_q \in (G)$. If $u_p - v_q = 0$, then we are done; otherwise $u_p - v_q \neq 0$ and we extend one of these two derivations. Since there are no infinite descending derivations (a basic property of admissible orderings), this process must stop.

QED

Corollary 5 *If $w \overset{*}{\rightarrow} w' \,(\mathrm{mod} S)$ and w is an assertion of S then w' is also an assertion.*

Proof

We know that $w \overset{*}{\rightarrow} w' \,(\mathrm{mod} S)$ iff $w' - w \in (G)$. The above lemma then implies that for some u, $w \overset{*}{\rightarrow} u$ and $w' \overset{*}{\rightarrow} u$, both $(\mathrm{mod} S)$. Hence $w \overset{*}{\rightarrow} u \overset{*}{\leftarrow} w'$.

QED

Remarks

It is interesting that Thue ideals are generalizations of monomial ideals since rules of the form $\alpha \rightarrow 0$ translates to monomials. Let us call a Thue polynomial that is not a monomial *proper*, and the ideals generated by proper Thue polynomials are called *proper Thue ideals*. Then it is not hard to see that a proper Thue ideal has a Gröbner basis consisting of proper Thue polynomials.

5 The Lower Bound based on S_0

We prove the following results about the system S_0.

Theorem 2 *Let $F_0 = F_{S_0}$ be the set of Thue polynomials corresponding to S_0, and G_0 the reduced Gröbner basis for F_0 with respect to some degree-compatible admissible ordering $\lesssim_A$. Then there is some $f \in G_0$ with $\deg(f) \geq e(n-1)$.*

We prove three more lemmas.

Let W_{n-1} be the set of all assertions divisible by $F_{n-1}[\mathtt{dec}]$. Define an equivalence relation $\sim$ on W_{n-1} where $w \sim w'$ if there is a derivation from w to w' involving only assertions in W_{n-1}.

For any two words w, w', and $k = 0, \ldots, n$ define

$$\mathtt{diff}_k(w, w') := \max\{\deg_k(\frac{w}{w''}), \deg_k(\frac{w'}{w''})\}$$

where $w'' = GCD(w, w')$. Furthermore,

$$\mathtt{diff}(w, w') := \max\{\mathtt{diff}_k(w, w') : k = 0, \ldots, n\}.$$

Clearly, $w \rightarrow w' \ (\mathrm{mod} S)$ implies some rule $r = (\alpha, \beta) \in S$ has size $\geq \mathtt{diff}(w, w') \geq \mathtt{diff}_k(w, w')$.

Recall the assertion $w_\infty = Q_{\mathtt{finish}} F_{1,n}[\mathtt{dec}] F_n[\mathtt{inc}] A_n^{e(n)}$.

Lemma 6 *If $w \in W_{n-1}$ and w is not $\sim$-equivalent to w_∞ then $\mathtt{diff}_n(w, w') \geq e(n-1)$.*

Proof

Pick $w^* \in W_{n-1}$ such that $w^* \sim w$ and $\mathtt{distance}(w_0, w^*)$ is minimal. This w^* is unique. Let w' be the parent of w^* in the tree T_0. Then the transition $w' \rightarrow w^*$ must come from applying $(\mathrm{F3})_{n-1}$. Moreover, w is not $\sim$-equivalent to w_∞ implies this transition is a mistake. This means $\deg_{A_{n-1}}(w^*) \geq 1$. Since no more application of $(\mathrm{F1\text{-}3})_{n-1}$ can take place after $w^*, \deg_{A_{n-1}}(w) \geq 1$.

Applying the Value Lemma to w gives us $\deg_n(w) = e(n) - \deg_{A_{n-1}}(w) \cdot e(n-1) \leq e(n) - e(n-1)$. The result follows since $\deg_n(w_\infty) = e(n)$.

QED

Lemma 7 *If* $w \neq w_\infty$ *and* $w \sim w_\infty$ *then* $\deg(w) > \deg(w_\infty)$.

Proof

Since $\deg_n(w) = \deg_n(w_\infty)$, it suffices to show that for some $k = 0, \ldots, n-1, \deg_k(w) > \deg_k(w_\infty) = 0$.

If $F_k[\mathtt{pass}] \mid w$ ($\mathtt{resp.}Q_{\mathtt{start}} \mid w$) then $\deg_k(w) = e(k)$ ($\mathtt{resp.}\deg_0(w) = d$), and we are done. Otherwise, for some $k = 1, \ldots, n$ we must have

$$Q_{\mathtt{finish}} F_{1,k}[\mathtt{dec}] F_k[\mathtt{inc}] \mid w.$$

Now $k = n$ is impossible since (by a corollary to the Value Lemma) this would mean $w = w_\infty$. Similarly, $k = n-1$ is not possible since $F_{n-1}[\mathtt{dec}] \mid w$. But if $k < n-1$ then by the Value Lemma, we must have $\deg_k(w) = e(k) > 0$.

QED

Lemma 8 *Let* w *be an assertion distinct from* w_∞. *If* $\deg(w) \leq \deg(w_\infty)$ *then* $\mathtt{diff}(w, w_\infty) \geq e(n-1)$.

Proof

We have three cases to consider.

Case $F_{n-1}[\mathtt{dec}] \mid w$:

It is not possible that $w \sim w_\infty$ since this implies $\deg(w) > \deg(w_\infty)$. But we had shown that if w is not $\sim$-equivalent to w_∞ then $\mathtt{diff}_n(u_1 u_2) \geq e(n-1)$.

Case $F_{n-1}[\mathtt{pass}] \mid w$:

Then by the Value Lemma $\deg_{n-1}(w) = e(n-1)$ and so $\mathtt{diff}_{n-1}(w, w_\infty) \geq e(n-1)$.

Case $F_{n-1}[\mathtt{inc}] \mid w$:

By the Value Lemma, $\deg_n(w) = V_w(n, n) = 0$. Hence $\mathtt{diff}_n(w, w_\infty) \geq e(n)$.

QED

The proof of theorem 2 is now rather simple. Since $w_0 \lesssim_A w_\infty$ and $w_\infty - w_0 \in (G_0)$, there are descending derivations

$$w_\infty \to u_1 \to \cdots \to u_p \,(\mathrm{mod} S_0)$$
$$w_0 \to v_1 \to \cdots \to v_q \,(\mathrm{mod} S_0)$$

with $p \geq 1$ and $u_p = v_q$. (Actually one can show that $u_p = w_0 = v_q$.) By the last lemma $\mathtt{diff}(w_\infty, u_1) \geq e(n-1)$. Hence the rule of S_0 that caused the transition $w_\infty \to u_1$ has size $\geq e(n-1)$. This implies our theorem.

6 Main Result

The system S_0 is not quite what we want because it has rules whose sizes are $d + O(n)$ rather than $d + O(1)$. We now transfer the theorem proved in the preceding section to a suitable Thue system S_1'.

Recall from Yap [8] the system S_1 in which S_0 is embedded. Using the $(n+1)$ additional variables $L_0, \ldots, L_n$, the rules of S_1 are an "expansion" of those in S_0. We reproduce the rules of S_1 next, for convenience. The following five rules replace (S1)-(S3):

$$\begin{array}{lllll}
\text{(T1)} & L_0 & \xrightarrow{Q_{\mathtt{start}} A_0} & L_1 & \\
\text{(T2)} & L_k & \xrightarrow{Q_{\mathtt{start}} F_k[\mathtt{pass}] A_0} & L_{k+1} & (k = 1, \ldots, n-1) \\
\text{(T3)} & L_k A_0 & \xrightarrow{Q_{\mathtt{start}} F_k[\mathtt{inc}]} & L_0 B_0 A_k^d & (k = 1, \ldots, n) \\
\text{(T4)} & L_k B_k^d & \xrightarrow{Q_{\mathtt{start}} F_k[\mathtt{dec}]} & L_0 B_0 & (k = 1, \ldots, n) \\
\text{(T5)} & Q_{\mathtt{start}} L_0 B_0^d & \longrightarrow & Q_{\mathtt{finish}} L_1 . &
\end{array}$$

Similarly, the finish rules (F1)-(F3) becomes, for $k = 1, 2, \ldots, n-1$:

$$\begin{array}{lllll}
\text{(G1)} & L_k F_k[\mathtt{dec}] & \xrightarrow{Q_{\mathtt{finish}}} & L_{k+1} F_k[\mathtt{inc}] & \\
\text{(G2)} & Q_{\mathtt{finish}} L_k F_k[\mathtt{inc}] & \longrightarrow & Q_{\mathtt{start}} L_0 A_0^d F_k[\mathtt{pass}] & \\
\text{(G3)} & Q_{\mathtt{finish}} L_k A_k & \xrightarrow{F_k[\mathtt{pass}]} & Q_{\mathtt{start}} L_0 A_0^d B_k & \\
\text{(G4)} & Q_{\mathtt{finish}} L_k F_k[\mathtt{pass}] A_k & \longrightarrow & Q_{\mathtt{start}} L_0 A_0^d F_k[\mathtt{dec}] B_k &
\end{array}$$

We will now embed S_1 in a new system S_1' using a trick mentioned in [8]: we replace the 4 variables of each level k

$$F_k[\mathtt{inc}], F_k[\mathtt{pass}], F_k[\mathtt{dec}], L_k$$

by two variables F_k, G_k. Recall that the set of well-formed words of S_1 was defined to be of the form $w = L_k w'$ where w' is a well-formed word of S_0 and $k = 0, \ldots, n$. Each well-formed word w of S_1 can be uniquely expressed in the form

$$w = u_0 u_1 \ldots u_n w'$$

where $u_k \in \{F_k[\mathtt{inc}], F_k[\mathtt{pass}], F_k[\mathtt{dec}], L_k\}^{\oplus}$ for $k = 1, \ldots, n$ and $u_0 \in \{L_0\}^{\oplus}$; furthermore, w' contains no occurrences of any flag or level variables. Call such u_k a *flag element* (at level k). Each u_k can be encoded by a word $\phi_k(u_k)$ of the form

$$F_k^i G_k^{5-i} \qquad (i = 0, \ldots, 5).$$

To be specific, we choose i such that i is odd iff $L_k \mid u_k$, and such that $\lfloor i/2 \rfloor = 0, 1$ or 2 according to whether $F_k[\mathtt{inc}], F_k[\mathtt{pass}]$ or $F_k[\mathtt{dec}]$ divides u_k. In case $k = 0$ we pretend that $F_0[\mathtt{inc}] \mid u_k$.

Then we define the map

$$\phi'(w) = \phi_0(u_0) \cdots \phi_n(u_n) w'.$$

The rules of the system S_1' can now be described. The rules (T1-5), (G1-4) of S_1 each involves flags and level variables from exactly two levels. Each such rule can be "elaborated" so that both the left and right hand sides now involve flag elements at these two levels. Furthermore, each rule has at most three possible "elaborations". For instance, (T1) can be elaborated in three ways into the form:

$$L_0 F_1[\mathtt{color}] \xrightarrow{Q_{\mathtt{start}}} L_1 F_1[\mathtt{color}]$$

for $[\mathtt{color}] \in \{[\mathtt{inc}], [\mathtt{pass}], [\mathtt{dec}]\}$. The corresponding rules for S_1' are

$$F_0 G_0^4 G_1^5 \xrightarrow{Q_{\mathtt{start}}} G_0^5 F_1 G_1^4$$

$$F_0 G_0^4 F_1^2 G_1^3 \longrightarrow G_0^5 F_1^3 G_1^2$$

$$F_0 G_0^4 F_1^4 G_1^1 \longrightarrow G_0^5 F_1^5$$

Similarly (T2), (T5) and (G1) can be elaborated 3 ways each. Rules (T3-4) and (G2-4) have each a unique elaboration. This completes our description of S_1'. It is clear that S_1' has $4n + O(1)$ variables and $O(n)$ rules each of size $d + O(1)$. Recall that S_0 is embedded in S_1 via the map: $\phi(w) = L_k w$ with $k = 0$ if $Q_{\mathtt{start}} \mid w$ and $k = 1$ otherwise. Hence S_0 is embedded in S_1' with the map ϕ_1 given by $\phi_1(w) = \phi'(\phi(w))$.

By definition of embedding, the fact that any simple derivation $w_0 \xrightarrow{*} w$ in the system S_0 is uniquely determined by w implies that any simple derivation $\phi_1(w_0) \xrightarrow{*} \phi(w)$ in the system S_1' is also uniquely determined by $\phi(w)$. It follows that the set of assertions of S_1' also forms a tree T_1' rooted at $\phi_1(w_0)$.

As usual, any assertion of S_1' of the form $\phi_1(w)$, w an assertion of S_0, is called *standard*. Since ϕ_1 is one-one, the inverse map $\phi_1^{-1}(w')$ is well defined if w' is a standard assertion. We extend the definition of ϕ_1^{-1} to include non-standard words as follows: If w' is non-standard, then there exists a unique forward transition $w_1 \rightarrow w_2 \ (\mathrm{mod} S_0)$ such that w' occurs in the unique simple derivation

$$\phi_1(w_1) \stackrel{*}{\rightarrow} \phi_1(w_2) \quad (\mathrm{mod} S_1').$$

We define $\phi_1^{-1}(w')$ to be w_1 in this case. Of course ϕ_1^{-1} is no longer one-one.

We note that following simple consequence of our rules:

(a) If w and w' are assertions of S_1' such that $\phi_1^{-1}(w) = \phi_1^{-1}(w')$ then $\deg(w) = \deg(w')$.

(b) $\deg(w) - 4(n+1) = \deg(\phi_1^{-1}(w))$.

We now prove the analogue of the last lemma in the previous section:

Lemma 9 *Let w be an assertion of S_1' distinct from $\phi_1(w_\infty)$. If $\deg(w) \leq \deg(\phi_1(w_\infty))$ then $\mathtt{diff}(w, \phi_1(w_\infty)) \geq \mathrm{e}(n-1)$.*

Proof

We note that $\deg(w) \leq \deg(\phi_1(w_\infty))$ iff $\deg(\phi_1^{-1}(w)) \leq \deg(w_\infty)$. Then by the last lemma in the previous section, $\mathtt{diff}(\phi_1^{-1}(w), w_\infty) \geq \mathrm{e}(n-1)$. The result follows since $\mathtt{diff}(w, \phi_1(w_\infty)) = \mathtt{diff}(\phi_1^{-1}(w), w_\infty)$.

QED

By exactly the same argument as before, we conclude that if G_1 is any Gröbner basis corresponding to S_1' then some polynomial in G_1 has degree $\geq e(n-1)$. Although the system S_1' has $4n+2$ variables, we can easily reduce this to $4n$ variables, at the expense of increasing the sizes of the rules (but with the sizes still $d + O(1)$).

7 Final Remark

It seems that one should be able to directly exploit the Thue system S_∞ in [8] which uses only $\sim 2n$ variables, thereby sharpening the lower bound proved here.

The next problem to be solved is to provide a lower bound that is independent of the choice of admissible orderings.

References

[1] Bruno Buchberger, "Gröbner bases: an algorithmic method in polynomial ideal theory", in *Recent Trends in Multidimensional Systems Theory*, (ed. N.K. Bose), D. Reidel Pub. Co. (1985).

[2] David Bayer and Michael Stillman, "On the complexity of computing syzygies", to appear, *J. of Symbolic Computation.*

[3] Thomas W. Dubé, "The structure of polynomial ideals and Gröbner bases", forthcoming Courant Institute report, and N.Y.U. PhD thesis.

[4] Dung T. Huynh, "A superexponential lower bound for Gröbner bases and Church-Rosser commutative Thue systems", *Information and Control* 68 (1986) 196-206.

[5] Ernst W. Mayr and Albert R. Meyer, "The complexity of the word problems for commutative semigroups and polynomial ideals", *Advances in Mathematics* 46 (1982) 305-329.

[6] Bud Mishra and Chee K. Yap, "Notes on Gröbner bases", Courant Institute - New York University, Robotics Laboratory Report No. 87, Nov. 1986. (To appear, special issue of *International Journal of Information Science*).

[7] H. Michael Möller and Ferdinando Mora, "Upper and lower bounds for the degree of Gröbner bases", Eurosam 84, *Lecture notes in Computer Science No. 174*, 172-183.

[8] Chee K. Yap, "A new lower bound construction for the word problem for commutative Thue systems", Technical report, September 1988, (RISC-LINZ), Johannes Kepler Universität Linz, Austria.

NYU COMPSCI TR-415
Yap, Chee-Keng
A double exponential lower
bound for degree-
compatible... c.2